UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/694,824	10/29/2003	Antonio Lain	200205659-2	7594

22879   7590   10/15/2008
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER
GERGISO, TECHANE

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
10/15/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>06/30/2008</u>.
2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>-14</u> is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) <u>1,2,5 and 8-14</u> is/are rejected.
7)☒ Claim(s) <u>3, 4, and 7</u> is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☒ All   b)☐ Some * c)☐ None of:
        1.☒ Certified copies of the priority documents have been received.
        2.☐ Certified copies of the priority documents have been received in Application No. _____.
        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

DETAILED ACTION

1.   This is a Final Office Action in response to the applicant's communication filed on June 30, 2008.

2.   Claims 1-14 have been examined and are pending. Claims 1, 2, 5, and 8-14 are rejected. Claims 3, 4, 6 and 7 are objected to.

Response to Arguments

3.   Applicant's arguments filed on June 30, 2008 have been fully considered but they are not persuasive.

4.   Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

5.   In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

    The applicant argues that Schenk fails to teach "issuing keys to users from subtrees within the hierarchy upon the basis of their grouping." (See page 5: applicant's argument). On the same page, contrary to the argument the applicant admits that "Specifically, Schwenk teaches

issuing each individual customer a cryptographic key from a system operator or TV program provider (column 3, lines 25-27), and then generating group keys for each subset (column 3, lines 40-42) and transmitting the group keys with the help of the cryptographic keys (column 3, lines 42-47). The group keys can be calculated by the user by using their individual cryptographic keys (column 3, lines 48,-51)". From the above citation and applicant's argument, it is clear that the applicant's analysis is incorrect, because group keys are calculated by the user using individual keys. User are formed in to groups and in order to achieve authorization, group keys are formed and keys are assigned to the users in a group. User groups and keys are formed in hierarchical level

(See Schwenk paragraph 3: lines 35-45: For example, let us assume that only customers 1, 2, 3, and 4 are authorized to receive the TV program, but not customer 5. In order to achieve this distribution of authorizations, customers 1 through 4 are grouped in the next higher hierarchical level--i.e., the second level preferably to form two subsets with two customers each. In practice this is accomplished by first generating group keys GK_1 and GK_2 for the two subsets at a central location. Group key GK_1 is transmitted with the help of the two individual cryptographic keys PK_1 and PK_2 of customers 1 and 2, whereas group key GK2 is transmitted with the help of the two individual cryptographic keys PK_3 and PK_4 of customers 3 and 4."

Therefore Schwenk teaches "issuing keys to users from subtrees within the hierarchy upon the basis of their grouping."

The applicant also argues that "there is no teaching or suggestion that the subsets are indicative of a level of service provider of the level of service to which the user is entitled." Again the examiner disagrees with the applicant's analysis because the user groups are formed and group keys are distributed to group members or users and when groups are formed they are based on privileges or authorization required for group members or users are entitled for. Thus the user groups and the user group keys are indicative of the a level of service provider of the level of service to which is the group user is entitled.

Therefore, for the above reasons, the applicant's arguments are not persuasive to overcome the prior arts in record and place independent claims 1, 10, 13 and 14 in condition for allowance. Dependent claims 2-9, 11 and 12 depending directly or indirectly from their corresponding independent claims are also not placed in condition for allowance based on their dependency.

Claim Rejections - 35 USC § 103

6.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7.   Claims 1, 2, 5 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schwenk (US Pat. No.: 6, 222, 923) in view of Kitaya et al. (hereinafter referred to as Kitaya, US Pat. No.: 7,269,257).

As per claims 1 and 13:

Schwenk discloses a method and computer entity adapted to managing security keys generated from a tree-structured ancestral hierarchy and issued by or on behalf of a service provider in order to provide selective access to provision of a service, wherein invalidation of a key necessitates reconfiguration of each other key within the hierarchy to the extent another key and an invalidated key share common ancestry, the method comprising the steps of (**features of the invention in the preamble are <u>not</u> given patentable weight during examination**. The examiner suggests to incorporate features of the invention from the preamble into body of the claims):

> defining at least two groups of users of the service (column 3: lines 35-48; column 4: lines 41-55);
>
> allocating within the hierarchy a distinct sub-tree domain for each group of users (column 3: lines 48-51); and
>
> issuing keys to users from sub-trees domains within the hierarchy upon the basis of their grouping (column 4: lines 17-38).

Schwenk does not explicitly disclose the sub-tree domains in the hierarchy are distinct. Kitaya, in analogous art, however, teaches the sub-tree domains in the hierarchy are distinct (column 3: lines 43-61; column 4: lines 25-33). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Schwenk to include the sub-tree domains in the hierarchy are distinct. This

modification would have been obvious because a person having ordinary skill in the art would have been motivated to provide an information processing system and an information processing method using an encryption key block, and a program distributing medium, which enables transmission of data safely to a valid user without relying on mutual authentication processing between a transmitter and a receiver of data as suggested by Kitaya in (column 3: lines 22-29).

As per claim 2:

Kitaya discloses method, wherein the at least two groups of users are defined upon the basis of a predetermined policy which provides that users are grouped according to their perceived value to a provider of the service (Figure 37A-D; Entity-Ann:3710, Entity-Bnk:3720.

As per claim 5:

Kitaya discloses method, wherein the ancestral hierarchy has a binary tree architecture (figure 3).

8.   Claims 8-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schwenk (US Pat. No.: 6, 222, 923) in view of Kitaya et al. (hereinafter referred to as Kitaya, US Pat. No.: 7,269,257)in further view of Wajs et al. (hereinafter referred to as Wajs, US Pat. No.: 7,155,611).

As per claim 8:

Schwenk and Kitaya do not explicitly disclose varying levels of service are available and a group of users of a low-service level are allocated dummy keys providing no security, thereby to obviate a need to reconfigure other user's keys upon their invalidation. Wajs, in analogous art, however, teaches varying levels of service are available and a group of users of a low-service level are allocated dummy keys providing no security, thereby to obviate a need to reconfigure other user's keys upon their invalidation (column 3: lines 43-61; column 4: lines 25-33). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Schwenk and Kitaya to include varying levels of service are available and a group of users of a low-service level are allocated dummy keys providing no security, thereby to obviate a need to reconfigure other user's keys upon their invalidation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to provide a conditional access system for broadcast applications, said conditional access system comprising a number of subscribers, each subscriber having a terminal including a conditional access module and a secure device for storing entitlements as suggested by Wajs in (column 1: lines 51-57).

As per claim 9:

Kitaya discloses a method, wherein the service is a dynamic service and its value is ephemeral and based upon its contemporaneous nature (column 7: lines 15-25).

9.   Claims 10-11 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Schwenk (US Pat. No.: 6, 222, 923) in view of Wajs et al. (hereinafter referred to as Wajs, US

Pat. No.: 7,155,611).

As per claims 10 and 14:

Schwenk discloses a method and computer entity adapted to managing security key

distribution to a plurality of users of a service comprising the steps of:

defining levels of service provision (column 3: lines 35-48; column 4: lines 41-55);

allocating keys to users which are indicative to a service provider of the level of service

        to which they are entitled (column 3: lines 48-51).

Schwenk does not explicitly disclose for at least one level of service provision, allocating

dummy keys which do not provide security for the provision of the service. Wajs, in analogous

art, however, teaches for at least one level of service provision, allocating dummy keys which do

not provide security for the provision of the service (column 3: lines 43-61; column 4: lines 25-

33). Therefore, it would have been obvious to a person having ordinary skill in the art at the

time the invention was made to modify the method disclosed by Schwenk to include for at least

one level of service provision, allocating dummy keys which do not provide security for the

provision of the service. This modification would have been obvious because a person having

ordinary skill in the art would have been motivated to provide a conditional access system for

broadcast applications, said conditional access system comprising a number of subscribers, each

subscriber having a terminal including a conditional access module and a secure device for storing entitlements as suggested by Wajs in (column 1: lines 51-57).

As per claim 11:

Wajs discloses a method, wherein method according to claim 10 wherein the placebo keys operate in such a manner that a user is not able to perceive a difference between a functioning security key and a dummy key (column 3: lines 43-61; column 4: lines 25-33).

Allowable Subject Matter

10.   Claims 3-4 and 6-7 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

11.   The following is a statement of reasons for the indication of allowable subject matter:

Claim 3 includes the following features of a digital signal recording disc and its corresponding methods, which are not taught or further suggested and would not have been obvious over prior arts of record and these features are: a first user group having the highest perceived value to the provider are allocated keys from a first sub-tree, and wherein keys from the first sub-tree share fewer ancestors with keys from other sub-trees than said keys from other sub-trees share with each other and keys from the first sub-tree share only one ancestor with said keys from other sub-trees.

Claim 6 includes the following features of a digital signal recording disc and its corresponding methods, which are not taught or further suggested and would not have been obvious over prior arts of record and these features are: the at least two groups of users are defined upon the basis of a predetermined policy which provides that users are grouped according to a perceived susceptibility of them ceasing to require the service, and a first user group having the highest perceived susceptibility are allocated keys from a first sub-tree, and wherein keys from the first sub-tree domain share fewer ancestors with keys from other sub-trees domains than said keys from other sub-trees domains share with each other; the service is a dynamic service and its value is ephemeral and based upon its contemporaneous nature.

Conclusion

12.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See the notice of reference cited in form PTO-892 for additional prior art.

13.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,
however, will the statutory period for reply expire later than SIX MONTHS from the mailing
date of this final action.

Contact Information

14.   Any inquiry concerning this communication or earlier communications from the
examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784
and fax number is (571) 273-3784. The examiner can normally be reached on 9:00am - 6:00pm.
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,
Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization
where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status information

for unpublished applications is available through Private PAIR only. For more information

about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access

to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197

(toll-free).

/T. J. G./
Primary Examiner, Art Unit 2437

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2437